

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 A Residence Located in Everett, Washington,  
 A Silver Ford Ecosport, and a Person,  
 more fully described in Attachments A-1 to A-3

Case No. MJ22-238

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Residence, Vehicle, and Subject as described in Attachments A-1 to A-3, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

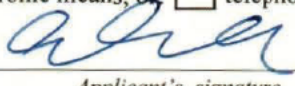
Code Section	Offense Description
18 U.S.C. § 2261A(2)(B)	Cyberstalking
47 U.S.C. § 223(a)(1)E	Repeated Harassing Communications

The application is based on these facts:

- ☒ See Affidavit of NCIS Special Agent Eddy D. Crochetiere, attached hereto and incorporated herein by reference.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

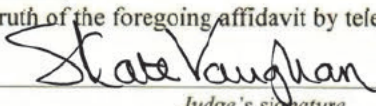
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or ☐ telephonically recorded.

  
Applicant's signature

Eddy D. Crochetiere, Special Agent, NCIS  
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/27/2022

  
Judge's signature

City and state: Seattle, Washington

S. KATE VAUGHAN, United States Magistrate Judge  
Printed name and title

# AFFIDAVIT OF EDDY D. CROCHETIERE

STATE OF WASHINGTON           )  
  )         SS  
COUNTY OF KING               )

I, Eddy D. Crochetiere, being first duly sworn on oath, depose and say:

## INTRODUCTION AND AGENT BACKGROUND

1. I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

2. I am a Special Agent (SA) with the Naval Criminal Investigative Service currently assigned to the Southwest Field Office in San Diego, California, and have been so employed since December 2020. In that capacity, I investigate all felony-level crimes against persons but specialize in Family and Sexual Violence (F&SV) and other associated offenses. Prior to my employment with NCIS, I served on active duty in the U.S. Coast Guard for over five years, where I worked as a Maritime Enforcement Specialist enforcing general federal law as well as recreational boating, commercial fishing, customs, and maritime security laws and regulations. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. My training and experience includes, but is not limited to, six months of rigorous training at FLETC in criminal investigations and the study of laws related to the United States Code. Additionally, I completed three months of rigorous training at FLETC in maritime criminal investigation and interdiction and the study of laws related to the United States Code, Code of Federal Regulations, and United Nations Convention on the Law of the Sea. I graduated from the University of California and Arizona State University where I obtained a Bachelor of Arts and a Master of Arts degree, respectively.

4. During my law enforcement career, I have become familiar with investigations of F&SV offenses (primarily domestic violence, rape, sexual assault, and child exploitation) and the methods by which offenders utilize electronic service providers to perpetrate peripheral offenses such as cyber stalking, criminal threats, harassing communications, obstruction of justice, destruction of evidence, witness intimidation, and the unauthorized distribution of intimate images. I have participated in the execution of numerous search warrants, including residential search warrants. As the vast majority of these have involved crimes completed using electronic communications services, I have personally been involved in the seizure of electronic devices. In executing my maritime law enforcement duties in the U.S. Coast Guard, I conducted searches of many dozens of seagoing residences and living compartments for contraband and other evidence of criminal activity. Based on my training, experience, and conversations with other experienced F&SV investigators, I have gained experience in the techniques and methods used by offenders to perpetrate and/or conceal their crimes, including conducting searches and seizures of both physical and digital evidence.

5. The facts set forth in this affidavit arise from my personal and direct participation in the investigation, my experience and training as an NCIS Special Agent, my conversations with witnesses, and my review of relevant documents and reports. I have not included each and every fact known to me or other investigative personnel concerning this investigation. My specialized training and experience in F&SV investigations, as well as the assistance and input of experienced fellow investigators, form a basis for my opinions and conclusions, which I drew from the facts set forth herein.

## PURPOSE OF THIS AFFIDAVIT

6. I make this affidavit in support of an application for a warrant authorizing the search of the following premises, further described below and in Attachment A-1, for evidence and instrumentalities, as further described in Attachment B, of the crimes of

cyberstalking, in violation of 18 U.S.C. § 2261A(2)(B), and repeated harassing interstate communications, in violation of 47 U.S.C. § 223(a)(1)(E) (the Target Offenses):

**Target Residence 1 (“TR1”)**, a residence located at **8620 8th Avenue West, Apartment C, Everett, WA 98204**. TR1 is the apartment designated as Apartment C within a light blue/gray-colored two-story four-unit apartment building with two garage doors facing the street on the west side of 8th Avenue West in Everett. The entrance to Apartment C is accessed by stairs to a door on the north side of the building and has a “C” on the door.

This application seeks authority to search extending to all parts of the premises under exclusive control of the subject of the investigation, Christopher Scott CRAWFORD (C.S. CRAWFORD), including the main residential unit, its assigned driveway and garage, any assigned storage structures, or outbuildings, curtilage, and all vehicles located in the same, and any containers, compartments, or safes located in the same, whether locked or not, where the items described in Attachment B (list of items to be seized) could be found.

7. This application also seeks warrants for the search of a vehicle known to be used by C.S. CRAWFORD, described in Attachment A-2, and for the search of the person of C.S. CRAWFORD, described in Attachment A-3.

8. As set forth below, there is probable cause to believe that aforementioned residence and vehicle, and the person of C.S. CRAWFORD contain items that are evidence of and have been used in furtherance of crimes by C.S. CRAWFORD, who is suspected of committing the offenses of cyberstalking and repeated harassing interstate communications, in violation of 18 U.S.C. § 2261A(2)(B) and 47 U.S.C. § 223(a)(1)(E), respectively.

## THE INVESTIGATION

9. On October 27, 2021, fourteen public-facing U.S. Navy email addresses received an email from the email address “crawford132@gmail.com,” with the display name of “Scott crawford.” As explained below, this email address is associated with subject C.S. CRAWFORD. The email contained thirty-six nude and/or intimate digital



1 | photos of a young woman later determined to be C.S. CRAWFORD's ex-wife K.C., a  
2 | U.S. Navy service member. The email message identified K.C. by name and rank and  
3 | alleged that she was a prostitute who solicited clients using the internet. I later confirmed  
4 | this email to be genuine through the use of an electronic search warrant to Google LLC  
5 | ("Google") for their original copy of the email from the "crawford132@gmail.com"  
6 | account. Routine criminal records checks revealed that C.S. CRAWFORD had an  
7 | extensive criminal history of stalking and threatening K.C. and those associated with her  
8 | in violation of existing restraining orders. The criminal history included numerous police  
9 | reports, several arrests, active restraining orders (in California, Texas, and Washington),  
10 | and active arrest warrants (in California and Texas). C.S. CRAWFORD is known to  
11 | reside in Everett, Washington, and K.C. was, at the time, stationed by the U.S. Navy in  
12 | San Diego, California. I have uncovered no information that would support the allegation  
13 | of prostitution.

14 |       10. I conducted an initial interview with K.C. on November 2, 2021. During the  
15 | interview, K.C. stated that, since their separation in approximately April of 2019,  
16 | C.S. CRAWFORD has continually harassed her with phone calls, text messages, emails,  
17 | social media messages, and gift messages appended to commercially delivered parcels, in  
18 | defiance of restraining orders. K.C. stated that C.S. CRAWFORD would call her  
19 | repeatedly – usually during inconvenient late-night hours – from his known cellular  
20 | phone number as well as Google Voice phone numbers unknown to her. K.C. stated  
21 | C.S. CRAWFORD's communications primarily contained profane and lewd insults,  
22 | disparaging remarks, and threats to "destroy" or "ruin" her. K.C. stated that  
23 | C.S. CRAWFORD has repeatedly told her that he would not stop harassing her until she  
24 | killed herself. K.C. has changed her phone number at least five times to avoid contact  
25 | with C.S. CRAWFORD but he very quickly discovers the new number and resumes  
26 | harassing her. In addition, K.C. stated C.S. CRAWFORD has told her that he provided  
27 | her contact information and address to his associates in prison.  
28 |

1           11. K.C. stated that C.S. CRAWFORD has harassed and threatened other  
2 people associated with her, including her mother, stepfather, grandfather, sister, divorce  
3 attorney, a court-mandated psychologist, and various members of her command.  
4 Interviews with or statements from her mother, stepfather, sister, court-mandated  
5 psychologist, and members of her command (including the individuals referred to herein  
6 as D.A. and M.N.) have confirmed the same.

7           12. K.C. stated she was also aware of C.S. CRAWFORD distributing her  
8 intimate images to her acquaintances and posting them on adult websites including the  
9 website Pornhub. K.C. stated she consensually sent C.S. CRAWFORD the intimate  
10 images approximately ten years prior. K.C.'s verbal descriptions of the photographs and  
11 their backgrounds matched the set of images sent to the U.S. Navy inboxes.

12           13. K.C. stated the harassment sends her "into a panic," causes her to not be  
13 able to "function," and has made her feel "anxious" and "paranoid." She stated she is  
14 "scared" of C.S. CRAWFORD and in the past has "slept with the recliner pushed up  
15 against the door" in case he were to break into her residence in the middle of the night.  
16 She added she is being treated by a therapist for Post-Traumatic Stress Disorder (PTSD)  
17 due to C.S. CRAWFORD's alleged offenses. During the in-person interview, I observed  
18 her to have visibly shaking hands, general fidgeting, dejected posture, shaky voice, and  
19 frantic speech patterns when discussing the offenses.

20           14. After the interview, K.C. provided me with a data CD containing  
21 approximately 246 digital files. These files consisted of portable document file (PDF)  
22 exports, audio files, screenshots, and images documenting hundreds of harassing emails,  
23 phone calls, text messages, social media messages, and voicemails appearing to be sent  
24 from C.S. CRAWFORD to K.C., her family members, and her associates. Almost every  
25 communication from C.S. CRAWFORD included insulting names, obscene language,  
26 threats, and/or statements of his intent to embarrass, humiliate, scandalize, stalk, "ruin,"  
27 "destroy," cause suffering to, cause mental illness to, and impoverish K.C.  
28

1 C.S. CRAWFORD also stated in several communications that he intended to torment  
2 K.C. until she killed herself.

3 15. I reviewed digital files obtained from K.C. documenting harassing text  
4 messages and transcribed voicemails from phone number (512) 667-5926 to K.C. Based  
5 on the content of the messages, they appeared to be from C.S. CRAWFORD, and  
6 subscriber information obtained from T-Mobile USA, Inc. for (512) 667-5926 revealed it  
7 to be subscribed to "CHRISTOPHER CRAWFORD" at 8616 8TH AVE W, EVERETT,  
8 WA 98204.

9 16. Based on my review of the digital files provided by K.C., the Google email  
10 account "crawford132@gmail.com," which is the same email account from which the  
11 nude/intimate photos of K.C. were sent to fourteen public-facing U.S. Navy email  
12 inboxes, was also the apparent sender of dozens of threatening and harassing emails to  
13 K.C. and others associated with her. The following are examples of email messages from  
14 "crawford132@gmail.com" that I have reviewed in the original submission of digital  
15 files by K.C. I later confirmed these emails to be genuine through the use of an electronic  
16 search warrant to Google for their original copy of the content of the  
17 "crawford132@gmail.com" account:

- 18 • An email sent on June 10, 2020, to K.C. and the guardian ad litem appointed by  
19 the Snohomish County Superior Court in connection with divorce proceedings,  
20 included the following: "You have a very hard road ahead of you and I'm going to  
21 be watching. One slip up, one instance of me thinking you are not fit to raise our  
22 daughter and Im going to take [S.C.<sup>1</sup>] away from you. That is a fucking promise."
- 23 • An email sent to K.C. on June 16, 2020, included the following: "I fucking hate  
24 you. The only things keeping me going are knowing that doing so vexes you and  
25 to someday watch you lose everything like I have."

---

26  
27  
28 <sup>1</sup> S.C. is the daughter of K.C. and C.S. CRAWFORD.

- 1 • An email sent to K.C. on June 22, 2020, included the following: “You wont be  
2 able to hide behind this TEMPORARY protective order for much longer.”
- 3 • An email sent to K.C. on October 27, 2021, included the following: “Why would  
4 you assume that your nude photos were only on one site? Every single time I miss  
5 my daughter, I am going to make you suffer for it. Ask [M.N.<sup>2</sup>] which one of your  
6 misshapen tits he likes best, hes seen them many times.”
- 7 • An email sent to K.C. on October 27, 2021, included the following: “and you have  
8 2 days to pay me 850 dollars AND have a visitation supervisor call me or I file 6  
9 contempt cases against you. You worthless fucking whore, I amgoing to make sure  
10 that you spend every single day hating that you were ever born.”
- 11 • A second email sent to K.C. on October 27, 2021, included the following: “and  
12 btw, I sent multiple copies of ALL your nudes to kirkland in prison and told him  
13 to distribute them to anyone he wanted. He also distributed your full name,social  
14 security number, address and employment...you know, in case anyone is getting  
15 out and wants to visit the cunt who he’s been jerking off to for a year.”
- 16 • An email sent to K.C. on October 29, 2021, included the following: “Just wanted  
17 to let you know that I came across a porn ad to “fuck local singles” and they were  
18 using one of your nudes in their ad. Isn’t that great?! Millions of people all over  
19 world, at random, now have proof that you are a whore for as long as their is the  
20 internet. Does it turn you on knowing that your father jerks off to you? Oh, did I  
21 forget to mention that I sent all of your nudes to your pedophile family years ago?  
22 Fuck you cunt. My goal in life is to make you kill yourself.”
- 23 • A second email sent to K.C. on October 29, 2021, included the following:  
24 “Tomorrow I’m going to sell your SSN, your phone number, your email address  
25 and all your personal history on the dark web. Just try and stop me, cunt.”  
26

---

28 <sup>2</sup> M.N. at the time was serving as K.C.’s Command Master Chief.



- 1 • A third email sent to K.C. on October 29, 2021, included the following: “I’m also  
2 going to print out your nudes and mail them to every address within 5 blocks of  
3 you, so all your neighbors know what a whore you are. I’m also working on  
4 getting the email addresses for every chief in your command and guess what they  
5 will find in their email? That’s right! Vulgar photos of a lying, cheating whore!”
- 6 • Another email sent to K.C. on October 29, 2021, included the following: “I am  
7 going to ruin your life. I am going to make every breath you have ever drawn,  
8 wasted. I am going to make sure you beg for a bus to run you over. And when  
9 your mental state starts slipping even more, I am going to fight tooth and nail to  
10 have you disgraced, comitted and then I am going to take S.C. from you forever.”
- 11 • An email sent on November 9, 2021, and forwarded directly to me from K.C.,  
12 included the following: “Keep trying, stupid, they wont stop me, they wont touch  
13 me, but they will absolutely arrest you for kidnapping. I know you think youve  
14 gotten me, im just letting you tighten the noose, cunt.”

15 17. An email sent from “crawford132@gmail.com” on November 30, 2021,  
16 and forwarded directly to me from K.C., consisted of the following: “If I end up homeless  
17 because of your bullshit, you will not survive my homelessness. I swear it.” I later  
18 confirmed this email to be genuine through the use of an electronic search warrant to  
19 Google for their original copy of the email from the “crawford132@gmail.com” account.  
20 K.C.’s subsequent reporting of this specific email to D.A., her supervisor, resulted in  
21 D.A. initiating an “expedited transfer” of K.C. and her daughter S.C. to a new duty  
22 station in a different state for her safety.

23 18. Subscriber information obtained from Google for  
24 “crawford132@gmail.com” revealed the email account to be subscribed to “Scott  
25 Crawford,” with a verified phone number of (512) 667-5926 and an account identifier of  
26 889486101222.

27 19. On November 24, 2021, Google was served with a preservation letter under  
28 18 U.S.C. § 2703(f) related to the Google email account “crawford132@gmail.com.”

20. Based on my review of emails provided to me by K.C.'s stepfather, on or about November 3, 2021, a Facebook account with the display name "Rick Johnston" was used to send to K.C.'s stepfather eight nude/intimate images of K.C. consistent with the set of intimate images sent by "crawford132@gmail.com" to the U.S. Navy inboxes. I later confirmed these messages to be genuine through the use of an electronic search warrant to Meta Platforms, Inc. (the parent company of Facebook) for their original copy of the content of the "Rick Johnston" Facebook account.

21. Information obtained from Meta Platforms, Inc. regarding the "Rick Johnston" Facebook account (account number 100074078874761) revealed the email address associated with the Facebook account to be the Google email account "rickjohnston1888@gmail.com." Subscriber information obtained from Google for the "rickjohnston1888@gmail.com." email account revealed Internet Protocol (IP) address 2601:601:a300:4ab0:cd57:98ec:2a4a:6899 was used to log in to this account on October 30, 2021, at 2:15 and 2:17 a.m. UTC. Subscriber information obtained from Comcast Cable Communications for this IP address revealed it to be subscribed to CHRISTOPHER CRAWFORD at 8620 8TH AVE W APT C, EVERETT, WA 98204-1640 (that is, **TR1**). Additionally, this same IP address was used to log into Instagram account number 27235979350 (with account vanity name "cscottcrawford") on October 30, 2021, at 4:02 a.m. UTC. Subscriber information regarding this Instagram account revealed it to be registered to "Scott Crawford" with the verified cellular phone number of (512) 667-5926.

22. I have received a copy of an Agreed Protective Order, number 2012-C1-15792, issued by the District Court of Bexar County, Texas, dated October 11, 2012, which protects K.C.'s mother, stepfather, and sisters from communication or harassing conduct by C.S. CRAWFORD. The order stemmed from an inconclusive police investigation into C.S. CRAWFORD's alleged sexual molestation of K.C.'s 10-year-old sister, C.B. The order states that it is in effect for the lifetime of C.S. CRAWFORD, states that C.S. CRAWFORD appeared at the hearing in person, was represented by an

1 attorney and agreed to the order, and is signed by C.S. CRAWFORD's attorney. The  
2 sending of the nude/intimate images of K.C. via the "Rick Johnston" Facebook account  
3 appear to be a violation of this order.

4 23. Based on my review of the digital files provided by K.C., the user of  
5 Google Voice phone number (401) 615-4218 has repeatedly called K.C.'s cellular phone  
6 and at least once has left a voicemail with disparaging remarks. Subscriber information  
7 obtained from Google for this Google Voice phone number revealed it to have the  
8 Google Account ID 889486101222, and to be registered to "Scott crawford" with a true  
9 phone number of (512) 667-5926. The same Google Account ID is also the account  
10 identifier for the "crawford132@gmail.com" Google email account.

11 24. Based on my review of the digital files provided by K.C., the Google Voice  
12 phone number (786) 904-3683 has sent lewd text messages to the cellular phone of J.M.,  
13 one of K.C.'s U.S. Navy coworkers. I have reviewed saved images of the text messages  
14 sent to J.M. The text messages contained lewd insults and two nude/intimate images of  
15 K.C. that appear to be from the set of nude/intimate images sent by  
16 "crawford132@gmail.com" to the U.S. Navy inboxes. Among other things, the sender of  
17 the messages stated, after sending one of the photos, "These pictures are being sent all  
18 over the navy, to her command, her coworkers, her former shipmates, even the secretary  
19 of defense." After sending another of the nude/intimate photos, the sender stated, "Don't  
20 worry, I don't care if you save the pics and jerk off to them...I sent her pictures and  
21 address to prison inmates for exactly that reason, and frankly, if I was married to your  
22 wife, I'd be looking everywhere else as well." After being advised by J.M. that if the  
23 sender continued to make contact with him or any member of his family, he would be  
24 contacting the police and filing a report for harassment and distributing pornographic  
25 images without consent, the sender responded by texting, among other things, "Call the  
26 cops, please, they won't do a fucking thing, just ask [K.C.] how much she was able to  
27 stop me." After threatening to ruin J.M.'s career, the sender replied, "And thanks to your  
28 empty shit talk, I am going to track down and contact every single member of your

1 family I can find.” Subscriber information obtained from Google for Google Voice phone  
2 number (786) 904-3683 revealed it to have Google Account ID 456326907605, and to be  
3 registered to “Christopher crawford” with a recovery email of  
4 “crawford132@gmail.com” and a recovery cellular phone number of (512) 667-5926.

5 25. Information obtained from Google revealed this Google Voice number  
6 called K.C.’s cellular phone three times and sent one text message on October 29, 2021. I  
7 have obtained a certified copy of a Criminal Protective Order issued by the Superior  
8 Court of California, County of San Diego, restraining C.S. CRAWFORD from having  
9 any personal, electronic, telephonic, or written contact with K.C., with exceptions only  
10 for the safe exchange of children and court-ordered visitation. The order indicates that  
11 C.S. CRAWFORD was served with a copy of the order at the hearing, and that it was  
12 issued on June 9, 2021, and expires three years from the date of issuance. At the time of  
13 the calls and text message in October 2021, the protective order was in effect, K.C. had  
14 custody of S.C. and was residing in California, and C.S. CRAWFORD was residing in  
15 Washington.

16 26. I have received and reviewed nine images and 28 digital audio files  
17 provided by U.S. Navy Master Chief Petty Officer M.N., who was, at the time, K.C.’s  
18 Command Master Chief. M.N. stated that he began receiving calls from  
19 C.S. CRAWFORD in approximately April 2021, and that the calls were initially polite  
20 until M.N. refused to assist C.S. CRAWFORD in forcing K.C. to provide money and  
21 other considerations, after which C.S. CRAWFORD began using obscene, lewd, and  
22 insulting language toward M.N. In one of the voicemail messages to M.N. that I have  
23 reviewed, the caller identified himself as “Christopher Crawford,” and said, in part, “I am  
24 not going to just burn down Petty Officer Crawford’s house, I’m going to burn down the  
25 house of everyone who gave her shelter...metaphorically speaking.” and “what do you  
26 fucking think I’m going to do to any of you that fucking let her do this shit to me? Any of  
27 you that step between me and my fucking child like that first command did, and I  
28 guarantee you I will make the act of Congress happen necessary to get your fucking

anchors in my god damned pocket!” In another voicemail message, the caller identified himself as “Chris Crawford” and said, in part, “Yeah, you keep going out and protecting her. And when she’s in prison, I’ll come after all of you next!” A portion of the images I reviewed documented text messages sent to M.N. from (512) 667-5926, the T-Mobile phone number associated with C.S. CRAWFORD. A sampling of the text messages from (512) 667-5926 that were sent to M.N.’s government cell phone read as follows:

- “Petty officer [K.C.], who bragged on the record about making chief, is an internet portn star and for the rest of her life, her friends, family and employers will receive links to the dozens of websites that contain her photos and videos and they all identify her by name, rank and rate.”
- “I’m going to make it so that her being in the military is a liability to the US government. I may even decide to list the classified material that the idiot left behind...who knows? Point is, as long as she has my daughter, she will live in hell.”
- “Point is, [K.C.] will be sending me 75% of her pay and retirement for the rest of her life. When she can no longer feed my daughter, I will take custody and watch happily as [K.C.] kills herself.”
- After sending a nude photo of K.C. that appears to be one of the photos sent to U.S. Navy inboxes, a text message was sent from the same number reading, “Did you enjoy the pictures? I’ve spent the last two days emailing them to every single navy email address I can get my hands on.”

27. The digital files from K.C. also documented text messages from (786) 904-3683, the Google Voice phone number associated with C.S. CRAWFORD. One of the images I reviewed appeared to be a string of undated text messages from (786) 904-3683 to M.N.’s personal cell phone. The sender sent an image file that appears to be one of the intimate photos of K.C. sent by C.S. CRAWFORD to U.S. Navy inboxes. After sending the photo, the sender sent several text messages that included the following:



- 1 • “Don’t worry, most of the navy around the world is receiving these
- 2 pictures”
- 3 • “I am going to destroy her and do everything I my power to make her kill
- 4 herself. I’ve already sent her nudes and address to some friends of mine in
- 5 prison, they are going to be visiting her for some fun when they get out, im
- 6 sure. I’m also selling her social, birthrate, name, address, and all military
- 7 paperwork I have from 10 years with her on the dark web.”

8 28. On December 15, 2021, Google was served with preservation letter under  
 9 18 U.S.C. § 2703(f) related to Google Voice phone numbers (401) 615-4218 and (786)  
 10 904-3683.

11 29. From my interview of K.C., I learned that her nude/intimate images were  
 12 posted to the Pornhub website by the Pornhub account with username “skabb155.”  
 13 Pursuant to a takedown request by K.C., Pornhub had later removed the images from  
 14 public view and banned the “skabb155” account from their service. I obtained Pornhub  
 15 subscriber information for the account “skabb155,” which revealed it to be registered to  
 16 “christopher crawford” with an email address “crawford132@gmail.com.” The subpoena  
 17 further revealed the account to have created two public photo albums: “US Navy, STG1,  
 18 San Diego” (Album ID 61386732), and “US NAVY STG1, San Diego” (Album ID  
 19 61386822). “STG1” is the U.S. Navy designation for K.C.’s rating, that is, Sonar  
 20 Technician (surface) Petty Officer 1st Class. I later obtained an electronic search warrant  
 21 for a copy of the content of the “skabb155” account from MG Freesites, Ltd., the parent  
 22 company that operates Pornhub, and confirmed that these two public photo albums  
 23 genuinely contained the same nude/intimate photos of K.C. that were sent to fourteen  
 24 public-facing U.S. Navy email inboxes by C.S. CRAWFORD.

25 30. On November 24, 2021, MG Freesites, Ltd. was served with a preservation  
 26 letter under 18 U.S.C. § 2703(f) related to the “skabb155” account.

27 31. Based on my interview of K.C. and my review of a digital photo provided  
 28 by her, a foot massager purchased from Amazon.com was delivered to K.C.’s residence

with a gift receipt bearing Order ID 111-4319768-1041835 and a transaction date of October 11, 2020, and stating it was from “c scott crawford.” The included gift message read, “Enjoy your gift! Happy early birthday. I hope this helps you relax so that you can focus on what is important and make better choices. I made promises I meant, even if you didn’t. From c scott crawford.” Subscriber information from Amazon for the purchaser associated with that Order ID number revealed the account that placed the order to be registered to “c scott crawford” with an email address of “crawford132@gmail.com” and a billing address of “8620 8TH AVE W APT C, EVERETT, WA, US 98204-1640” (that is, **TR1**). This communication came at a time when the Criminal Protective Order from San Diego County was in effect. I later confirmed this Amazon gift delivery to be genuine through the use of an electronic search warrant to Amazon.com, Inc. for their original copy of the data associated with Order ID 111-4319768-1041835.

32. On December 3, 2021, Amazon.com, Inc. was served with a preservation letter under 18 U.S.C. § 2703(f) related to order identifier 111-4319768-1041835 and the account associated with that transaction.

33. Based on my interview of K.C. and my review of digital files provided by her, the user of the Facebook account with display name “Scott Crawford” (account identifier 100002445195272) sent harassing messages to K.C. Among the messages I have reviewed were a string of messages sent to K.C. between 4:09 a.m. and 4:58 a.m. on January 09, 2020, that read as follows:

- “What’s worse, using words to hurt someone or using childish, petty, vindictive actions to do the same?”
- “‘People will provoke you until they bring your ugly side, then play the victim when you go there.’ You are not the victim, stop trying to be.”

I later confirmed these messages to be genuine through the use of an electronic search warrant to Meta Platforms, Inc. for their original copy of the content of the “Scott Crawford” Facebook account.

34. Additionally, based on the digital files provided by K.C., the “Scott Crawford” Facebook account also sent harassing messages to K.C.’s mother, J.C. that appear to be in violation of the lifetime restraining order against C.S. CRAWFORD issued by the District Court of Bexar County, Texas. I have reviewed a message from “Scott Crawford” to J.C. sent on August 1, 2020, that reads as follows (certain references to individuals have been replaced with bracketed references based on my understanding of these individuals’ identities):

call your daughter. she has left me so you have gotten what you always wanted. If I find out that you are talking to [S.C.] though, I will be calling CPS on [K.C.] for the 4th time. She is already going to lose custody of [S.C.], don’t help her do it any more thoroughly  
Dont forget that you are a pedophile, like your whole family. The [Guardian ad Litum for S.C.] has already ruled that you are a threat to [S.C.] and I have [K.C.’s] wills where she said she disowned you. YOu will never be allowed to be in a position where you can hurt my daughter like you did with your other kids, but you can still talk to your daughter.  
Granted, she has become a stupid, irresponsible, abusive, negligent, evil waste of life, but taht is why I feel you two will get along better now.

I later confirmed these messages to be genuine through the use of an electronic search warrant to Meta Platforms, Inc. for their original copy of the content of the “Scott Crawford” Facebook account.

35. According to Facebook subscriber records, the “Scott Crawford” Facebook account is registered to “Scott Crawford” with a verified phone number of (512) 667-5926 (verified on August 22, 2022), and a registered email address of crawford132@hotmail.com.

36. Based on my interview with K.C. and my review of digital files provided by her, the Facebook account with display name “Christopher Crawford” (account identifier 100054164457078) sent harassing messages to J.C. contemporaneously with the messages from the “Scott Crawford” account. Among other things, the messages accused J.C. of being a “pedophile” and claimed that K.C. was now a convicted criminal with over 30 more charges pending. Records checks conducted through the National

1 Crime Information Center (NCIC), State Regional & Federal Enterprise Retrieval System  
 2 III (SRFERS), and Department of Defense Law Enforcement Defense Data Exchange (D-  
 3 DEx) databases revealed no criminal history for K.C. A check conducted through the  
 4 Defense Information System for Security (DISS) database revealed K.C. remains eligible  
 5 for a Sensitive Compartmented Information (SCI) clearance designation, which is the  
 6 highest security clearance designation in the U.S. Government. According to Facebook  
 7 subscriber information, the “Christopher Crawford” account revealed is registered to  
 8 “Christopher Crawford” with a verified phone number of (512) 667-5926, and an account  
 9 creation date of August 1, 2020. I later confirmed these messages to be genuine through  
 10 the use of an electronic search warrant to Meta Platforms, Inc. for their original copy of  
 11 the content of the “Christopher Crawford” Facebook account.

12 37. On December 6, 2021, Meta Platforms, Inc. was served with a preservation  
 13 letter under 18 U.S.C. § 2703(f) related to Facebook account identifiers  
 14 100002445195272 (username Scott Crawford), 100054164457078 (username  
 15 Christopher Crawford), and 100074078874761 (username Rick Johnston).

16 38. Based on my interview with K.C. and my review of digital files provided  
 17 by her, the Instagram account “cscotterawford” (account identifier 27235979350) made a  
 18 harassing public comment on a public Instagram post made by K.C. The public comment  
 19 stated, “She wrote me this on 4/07/2018” along with a digital image appearing to be a  
 20 photograph of a computer screen displaying text. Among the text included the following,  
 21 purportedly a private message written by K.C. to C.S. CRAWFORD on a previous date,  
 22 reading, in part, “...about trying to make myself better and stronger, more decisive for  
 23 you and [S.C.]. I’m supposed to be the head of household and I can barely stand up for  
 24 myself or how many times I feel like I let you down because I don’t want to try  
 25 something new with you or that I wouldn’t let you treat me.” According to Facebook  
 26 subscriber information, this account is registered to “Scott Crawford” with a verified  
 27 phone number of (512) 667-5926.

39. Based on my interview with K.C. and my review of digital files provided by her, the Instagram account “im\_not\_broken\_just\_very\_sad” (account identifier 27605029014) sent multiple harassing messages to K.C. and public comments on her posts. Among the messages I have reviewed, a string of messages sent to K.C. on January 1, 2020, included the following, apparently posted in the guise of an anonymous third party: “...he feels like his mother is emperor palpatine and you are anakin Skywalker. He feels like padme in the sense that you are turning to the dark side and it is breaking his heart. To side with her over him after everything she has done is almost too much for him to bear and the fact that you left [S.C.] with her instead of him is infuriating to him,” and “...from his point of view you are the aggressor, not the victim; you have everything and he is begging for mercy scraps. He truly feels manipulated and baited by you, he feels you played him and then betrayed ever promise you ever made to him.” I later confirmed these messages to be genuine through the use of an electronic search warrant to Meta Platforms, Inc. for their original copy of the content of the “im\_not\_broken\_just\_very\_sad” Instagram account. Among the public comments I have reviewed included the following, also written in the guise of an anonymous third party: “And I like how you say ‘time to grow’ like you are the same wrist cutting, medicated sex toy for a married couple, flunking out of college, wanting to get two full arm sleeves and a dozen piercings, sleeping with a husband and wife, your gay boyfriend, and then seducing your future husband by telling him you were single, that you were when scott first found you sleeping in the parking lot of the college. Good think you are away from him and can ‘grow,’” and “Good luck with a career as a sub hunter when you cant serve on a ship... You are not a good person. Everything you knew about being good came from him and like a 14 year old, hes no longer around so in your messed up head, nothing he ever said was true.” According to Facebook subscriber information, this account is registered to “scott crawford.” The email address associated with the account is “endless sadness15@gmail.com,” and the account was registered on January 1, 2020.



1           40. On December 6, 2021, Meta Platforms, Inc. was served with a preservation  
2 letter under 18 U.S.C. § 2703(f) related to Instagram account identifiers 27235979350  
3 and 27605029014.

4           41. On April 24, 2022, K.C. stated she believed C.S. CRAWFORD currently  
5 resided at 8620 8th Avenue West, Apartment C, Everett, WA 98204 (TR1) with a  
6 woman named “Jennifer.” This address is consistent with the mailing addresses registered  
7 for many of the aforementioned electronic communications service accounts. Between  
8 April 25, 2022, and May 10, 2022, NCIS agents conducted multiple instances of physical  
9 surveillance of TR1 and observed C.S. CRAWFORD entering and exiting the north door  
10 marked with a “C” in a manner consistent with someone who resides there. Agents  
11 additionally observed a woman believed to be “Jennifer” and another male entering and  
12 exiting the same apartment in a manner consistent with someone who resides there.

13           42. On May 10, 2022, NCIS agents conducting physical surveillance of TR1  
14 observed C.S. CRAWFORD exit the residence, get into the driver’s seat of a silver Ford  
15 EcoSport Sports Utility Vehicle (SUV) parked in the driveway, and drive away. The  
16 vehicle bore license plate number BPT0800. Records checks revealed the vehicle to be  
17 most recently registered to C.S. CRAWFORD, however the registration expired in June  
18 2021.

19                           **KNOWLEDGE BASED ON TRAINING & EXPERIENCE**

20           43. Based upon my training, experience, and participation in this and other  
21 investigations involving crimes completed using digital technology, my conversations  
22 with other experienced investigators with whom I work, I have learned and know the  
23 following.

24           44. I know that those who commit crimes completed using electronic  
25 communications services, including cyberstalking and/or harassing interstate  
26 communications, commonly maintain many accounts with numerous electronic service  
27 providers. Many of these accounts utilize pseudonyms or other false identifying  
28 information in order to obfuscate their true identity, convey to their victims an illusion of

1 conspiracy or pervasiveness, and create distance from their crimes. Due to these factors,  
2 investigators are rarely aware of the full range of a cyberstalker's activities until the  
3 instrumentalities are physically seized and their contents examined for previously  
4 unknown accounts and activity.

5 45. I know that those who commit cyberstalking and/or harassing interstate  
6 communications commonly use mobile computing devices such as smart phones in  
7 addition to traditional computers in order to perpetrate their crimes. They may prefer  
8 mobile computing devices because, first, many electronic communications services only  
9 make their services available on mobile computing device platforms. Second, they can be  
10 easily carried to permit the user maximum flexibility in selecting the time and place they  
11 can commit the offenses, as commonly the offenses involve frequent, repeated, and  
12 persistent communications.

13 46. Also, in my experience, it is very for individuals involved in such illegal  
14 conduct to use and maintain computers or mobile computing devices at their residences  
15 and/or vehicles, when not on their person. By nature of their design and operation,  
16 network equipment is generally required to remain in one's residence.

17 47. Based upon information learned during the investigation, I believe that  
18 C.S. CRAWFORD used computers and/or mobile computing devices as instrumentalities  
19 of the crimes of cyberstalking and harassing interstate communications. During my  
20 investigation, I have learned that C.S. CRAWFORD used various online services  
21 (Facebook, Instagram, Google, Amazon, and PornHub) to conduct his harassment of  
22 K.C. Therefore, I believe that evidence associated with these offenses is likely to be  
23 located in computers, mobile computing devices, networking hardware, and electronic  
24 storage media located in his residence or vehicle, or on his person.

25 **COMPUTERS, MOBILE DEVICES, ELECTRONIC STORAGE AND**  
26 **FORENSIC ANALYSIS**

27 48. As described above and in Attachment B, this application seeks permission  
28 to search for evidence and instrumentalities of cyberstalking and harassing interstate

communications that might be found in the locations to be searched, in whatever form they may be found. One form in which such evidence may be found is data stored on digital devices<sup>1</sup> such as computer hard drives or other electronic storage media.<sup>2</sup> Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media, or potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

49. I know that when an individual uses a computer or mobile computing device to conduct cyberstalking and harassing interstate communications, the individual's computer or mobile computing device will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. From my training and experience, I believe that a computer or mobile computing device used to commit a crime of this type may contain: data that is evidence of how the computer was used; data showing the identity of the person perpetrating the conduct; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

50. *Probable cause.* I submit that if a computer, mobile computing device, networking hardware, or electronic storage medium is found pursuant to a search authorized by the warrant, there is probable cause to believe evidence will be stored in that item, for at least the following reasons:

---

<sup>1</sup> As used herein, "digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

<sup>2</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1           a.       Based on my knowledge, training, and experience, I know that  
2 computer files or remnants of such files can be preserved (and consequently also then  
3 recovered) for months or even years after they have been downloaded onto a storage  
4 medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to  
5 any electronic storage medium can be stored for years at little or no cost. Even when files  
6 have been deleted, they can be recovered months or years later using readily available  
7 forensics tools. This is so because when a person “deletes” a file on a digital device or  
8 other electronic storage media, the data contained in the file does not actually disappear;  
9 rather, that data remains on the electronic storage medium until it is overwritten by new  
10 data.

11           b.       Therefore, deleted files, or remnants of deleted files, may reside in  
12 free space or slack space—that is, in space on the electronic storage medium that is not  
13 currently being used by an active file—for long periods of time before they are  
14 overwritten. In addition, a computer or mobile computing device’s operating system may  
15 also keep a record of deleted data in a “swap” or “recovery” file.

16           c.       Similarly, files that have been viewed via the Internet are typically  
17 automatically downloaded into a temporary Internet directory or “cache.” The browser  
18 often maintains a fixed amount of storage space devoted to these files, and the files are  
19 only overwritten as they are replaced with more recently viewed Internet pages or if a  
20 user takes steps to delete them.

21           d.       Wholly apart from user-generated files, computer storage media—in  
22 particular, computers’ internal hard drives—contain electronic evidence of how a  
23 computer has been used, what it has been used for, and who has used it. To give a few  
24 examples, this forensic evidence can take the form of operating system configurations,  
25 artifacts from operating system or application operation; file system data structures, and  
26 virtual memory “swap” or paging files. Computer users typically do not erase or delete  
27 this evidence, because special software is typically required for that task. However, it is  
28 technically possible to delete this information.

1 e. Home networking hardware such as “routers,” “switches,” and  
2 “modems” maintain extensive records of every computer or mobile computing device  
3 that has connected to the internet through it, in the form of logs documenting each  
4 computer or mobile computing device’s media access control (MAC) address  
5 (completely unique to that only that device, similar to a serial number) and the times,  
6 dates, and general activity of that computer or mobile computing device. This can  
7 provide information about who was in control of specific account activity using a specific  
8 computing device at a particular date and time.

9 51. Based on my training and experience, the data maintained in a mobile  
10 computing device used by a person committing cyberstalking is often evidence of a crime  
11 or crimes. This includes the following:

12 a. The assigned number to a smart phone (known as the mobile  
13 directory number or MDN), and the identifying telephone serial number (International  
14 Mobile Equipment Identity, or IMEI) are important evidence because they reveal the  
15 service provider, allow us to confirm subscriber information, and uniquely identify the  
16 telephone. This information can be used to confirm if the smart phone was the computing  
17 device logging into certain target electronic communications service accounts at certain  
18 times.

19 b. The stored list of recent received and sent calls is important  
20 evidence. It identifies telephones recently in contact with the smart phone user. This is  
21 valuable information in this investigation because it can demonstrate that the subject of  
22 the investigation was attempting to contact known victims of his suspected stalking and  
23 harassing interstate communications and/or identify additional victims that were  
24 previously unknown. Additionally, logs and time stamps of outgoing calls can  
25 demonstrate the communications were of a repeated nature and/or were initiated at  
26 inconvenient, bothersome hours.

27 c. Stored text messages are important evidence, similar to stored phone  
28 numbers. Agents can identify both known and previously unknown victims. Additionally,



1 due to the nature of cellular telephone service provider's business operations, the  
2 providers rarely retain the content of text messages and therefore that data is only  
3 obtainable through control of the actual device.

4 d. The software applications loaded on a mobile computing device are  
5 also important evidence. Beyond simply confirming that the subject of the investigation  
6 utilizes the same electronic communications services as were used to perpetrate the  
7 criminal offenses, most software applications indicate previously-utilized accounts when  
8 opened. This can link the bearer of the mobile computing device to specific accounts that  
9 are known to be involved in the alleged criminal activity.

10 52. *Forensic evidence.* As further described in Attachment B, this application  
11 seeks permission to locate not only computer files that might serve as direct evidence of  
12 the crimes described on the warrant, but also for forensic electronic evidence that  
13 establishes how digital devices or other electronic storage media were used, the purpose  
14 of their use, who used them, and when. There is probable cause to believe that this  
15 forensic electronic evidence will be on any digital devices or other electronic storage  
16 media located during the search because:

17 a. Stored data can provide evidence of a file that was once on the  
18 digital device or other electronic storage media but has since been deleted or edited, or of  
19 a deleted portion of a file (such as a paragraph that has been deleted from a word  
20 processing file). Virtual memory paging systems can leave traces of information on the  
21 digital device or other electronic storage media that show what tasks and processes were  
22 recently active. Web browsers, e-mail programs, and chat programs store configuration  
23 information that can reveal information such as online nicknames and passwords.  
24 Operating systems can record additional information, such as the history of connections  
25 to other computers, the attachment of peripherals, the attachment of USB flash storage  
26 devices or other external storage media, and the times the digital device or other  
27 electronic storage media was in use. Computer file systems can record information about  
28 the dates files were created and the sequence in which they were created.

1           b. As explained herein, information stored within a computer and other  
2 electronic storage media may provide crucial evidence of the “who, what, why, when,  
3 where, and how” of the criminal conduct under investigation, thus enabling the United  
4 States to establish and prove each element or alternatively, to exclude the innocent from  
5 further suspicion. In my training and experience, information stored within a computer or  
6 storage media (e.g., registry information, communications, images and movies,  
7 transactional information, records of session times and durations, internet history, and  
8 anti-virus, spyware, and malware detection programs) can indicate who has used or  
9 controlled the computer or storage media. This “user attribution” evidence is analogous  
10 to the search for “indicia of occupancy” while executing a search warrant at a residence.  
11 The existence or absence of anti-virus, spyware, and malware detection programs may  
12 indicate whether the computer was remotely accessed, thus inculcating or exculpating the  
13 computer owner and/or others with direct physical access to the computer. Further,  
14 computer and storage media activity can indicate how and when the computer or storage  
15 media was accessed or used. For example, as described herein, computers typically  
16 contain information that log: computer user account session times and durations,  
17 computer activity associated with user accounts, electronic storage media that connected  
18 with the computer, and the IP addresses through which the computer accessed networks  
19 and the internet. Such information allows investigators to understand the chronological  
20 context of computer or electronic storage media access, use, and events relating to the  
21 crime under investigation. Additionally, some information stored within a computer or  
22 electronic storage media may provide crucial evidence relating to the physical location of  
23 other evidence and the suspect. For example, images stored on a computer may both  
24 show a particular location and have geolocation information incorporated into its file  
25 data. Such file data typically also contains information indicating when the file or image  
26 was created. The existence of such image files, along with external device connection  
27 logs, may also indicate the presence of additional electronic storage media (e.g., a digital  
28 camera or cellular phone with an incorporated camera). The geographic and timeline

1 information described herein may either inculcate or exculpate the computer user. Last,  
2 information stored within a computer may provide relevant insight into the computer  
3 user's state of mind as it relates to the offense under investigation. For example,  
4 information within the computer may indicate the owner's motive and intent to commit a  
5 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt  
6 (e.g., running a "wiping" program to destroy evidence on the computer or password  
7 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

8           d.       The process of identifying the exact files, blocks, registry entries,  
9 logs, or other forms of forensic evidence on a digital device or other electronic storage  
10 media that are necessary to draw an accurate conclusion is a dynamic process. While it is  
11 possible to specify in advance the records to be sought, digital evidence is not always  
12 data that can be merely reviewed by a review team and passed along to investigators.  
13 Whether data stored on a computer is evidence may depend on other information stored  
14 on the computer and the application of knowledge about how a computer behaves.  
15 Therefore, contextual information necessary to understand other evidence also falls  
16 within the scope of the warrant.

17           e.       Further, in finding evidence of how a digital device or other  
18 electronic storage media was used, the purpose of its use, who used it, and when,  
19 sometimes it is necessary to establish that a particular thing is not present. For example,  
20 the presence or absence of counter-forensic programs or anti-virus programs (and  
21 associated data) may be relevant to establishing the user's intent.

22       53.       Searching computer systems for the evidence described in Attachment B  
23 may require a range of data analysis techniques. In some cases, it is possible for agents  
24 and analysts to conduct carefully targeted searches that can locate evidence without  
25 requiring a time-consuming manual search through unrelated materials that may be  
26 commingled with criminal evidence. In other cases, however, such techniques may not  
27 yield the evidence described in the warrant. Criminals can mislabel or hide files and  
28 directories, encode communications to avoid using key words, attempt to delete files to

1 evade detection, or take other steps designed to frustrate law enforcement searches for  
2 information. These steps may require agents and law enforcement or other analysts with  
3 appropriate expertise to conduct more extensive searches, such as scanning areas of the  
4 disk not allocated to listed files, or peruse every file briefly to determine whether it falls  
5 within the scope of the warrant. In light of these difficulties, the Naval Criminal  
6 Investigative Service intends to use whatever data analysis techniques appear necessary  
7 to locate and retrieve the evidence described in Attachment B.

8       54. *Necessity of Seizing or Copying Entire Computers or Storage Media.* Based  
9 upon my knowledge, training and experience, I know that searching for information  
10 stored in computers often requires agents to seize most or all electronic storage devices to  
11 be searched later by a qualified computer expert in a laboratory or other controlled  
12 environment. This is often necessary to ensure the accuracy and completeness of such  
13 data, and to prevent the loss of the data either from accidental or intentional destruction.  
14 Additionally, to properly examine those storage devices in a laboratory setting, it is often  
15 necessary that some computer equipment, peripherals, instructions, and software be  
16 seized and examined in the laboratory setting. This is true because of the following:

17           a. *The volume of evidence.* Electronic storage media (like hard disks,  
18 optical disks, flash drives, or flash cards) can store the equivalent of millions of pages of  
19 information. Additionally, a suspect may try to conceal criminal evidence; he or she  
20 might store it in random order with deceptive file names. This may require searching  
21 authorities to peruse all the stored data to determine which particular files are evidence or  
22 instrumentalities of crime. This sorting process can take weeks or months, depending on  
23 the volume of data stored, and it would be impractical and invasive to attempt this kind of  
24 data search on-site.

25           b. *The time required for an examination.* As noted above, not all  
26 evidence takes the form of documents and files that can be easily viewed on site.  
27 Analyzing evidence of how a computer has been used, what it has been used for, and who  
28 has used it requires considerable time, and taking that much time on premises could be

1 unreasonable. As explained above, because the warrant calls for forensic electronic  
2 evidence, it is exceedingly likely that it will be necessary to thoroughly examine the  
3 respective digital device and/or electronic storage media to obtain evidence. Computer  
4 hard drives, digital devices and electronic storage media can store a large volume of  
5 information. Reviewing that information for things described in the warrant can take  
6 weeks or months, depending on the volume of data stored, and would be impractical and  
7 invasive to attempt on-site.

8           b.     *Technical requirements.* Searching computer systems for criminal  
9 evidence sometimes requires highly technical processes requiring expert skill and  
10 properly controlled environment. The vast array of computer hardware and software  
11 available requires even computer experts to specialize in some systems and applications,  
12 so it is difficult to know before a search which expert is qualified to analyze the system  
13 and its data. In any event, however, data search processes are exacting scientific  
14 procedures designed to protect the integrity of the evidence and to recover even “hidden,”  
15 erased, compressed, password- protected, or encrypted files. Because computer evidence  
16 is vulnerable to inadvertent or intentional modification or destruction (both from external  
17 sources or from destructive code imbedded in the system as a “booby trap”), a controlled  
18 environment may be necessary to complete an accurate analysis.

19           c.     *Variety of forms of electronic media.* Evidence sought under this  
20 warrant could be stored in a variety of storage media formats that may require off-site  
21 reviewing with specialized forensic tools.

22           55.    *Nature of Examination.* Based on the foregoing, and consistent with Rule  
23 41(e)(2)(B), I hereby request the Court’s permission to seize the computer hardware (and  
24 associated peripherals), mobile computing devices, networking hardware, and electronic  
25 storage media that are believed to contain some or all of the evidence described in the  
26 warrant, and to conduct an off-site search of the same for the evidence described, if, upon  
27 arriving at the scene, the agents executing the search conclude that it would be  
28 impractical to search the specified hardware on-site for this evidence. The off-site search



1 may require techniques, including but not limited to computer-assisted scans of the entire  
2 medium, that might expose many parts of a device to human inspection in order to  
3 determine whether it is evidence described by the warrant.

4       56. As with any search warrant, I expect that this warrant will be executed  
5 reasonably. Reasonable execution will likely involve conducting an on-scene  
6 investigation of what devices must be seized or copied.

7       57. *Biometric unlock.* The warrant I am applying for would permit law  
8 enforcement to obtain from certain individuals the display of physical biometric  
9 characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to  
10 unlock devices subject to search and seizure pursuant to this warrant. I seek this  
11 authority based on the following:

12           a. I know from my training and experience, as well as from  
13 information found in publicly available materials published by device manufacturers, that  
14 many electronic devices, particularly newer mobile devices and laptops, offer their users  
15 the ability to unlock the device through biometric features in lieu of a numeric or  
16 alphanumeric passcode or password. These biometric features include fingerprint  
17 scanners and facial recognition features. Some devices offer a combination of these  
18 biometric features, and the user of such devices can select which features they would like  
19 to utilize.

20           b. If a mobile computing device is equipped with a fingerprint scanner,  
21 a user may enable the ability to unlock the device through his or her fingerprints. For  
22 example, Apple offers a feature called “Touch ID,” which allows a user to register up to  
23 five fingerprints that can unlock a device. Once a fingerprint is registered, a user can  
24 unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which  
25 is found in the round button (often referred to as the “home” button) located at the bottom  
26 center of the front of the device. The fingerprint sensors found on devices produced by  
27 other manufacturers have different names but operate similarly to Touch ID. If a device is  
28 equipped with a facial recognition feature, a user may enable the ability to unlock the

1 device through his or her face. For example, Apple offers a facial recognition feature  
2 called “Face ID.” During the Face ID registration process, the user holds the device in  
3 front of his or her face. The device’s camera then analyzes and records data based on the  
4 user’s facial characteristics. The device can then be unlocked if the camera detects a face  
5 with characteristics that match those of the registered face. Facial recognition features  
6 found on devices produced by other manufacturers have different names but operate  
7 similarly to Face ID.

8           c.       In my training and experience, users of electronic devices often  
9 enable the aforementioned biometric features because they are considered to be a more  
10 convenient way to unlock a device than by entering a numeric or alphanumeric passcode  
11 or password. Moreover, in some instances, biometric features are considered to be a more  
12 secure way to protect a device’s contents. This is particularly true when the users of a  
13 device are engaged in criminal activities and thus have a heightened concern about  
14 securing the contents of a device.

15           d.       As discussed in this affidavit, based on my training and experience I  
16 believe that one or more digital devices will be found during the search. The passcode or  
17 password that would unlock the device(s) subject to search under this warrant is not  
18 known to law enforcement. Thus, law enforcement personnel may not otherwise be able  
19 to access the data contained within the device(s), making the use of biometric features  
20 necessary to the execution of the search authorized by this warrant.

21           e.       I also know from my training and experience, as well as from  
22 information found in publicly available materials including those published by device  
23 manufacturers, that biometric features will not unlock a device in some circumstances  
24 even if such features are enabled. This can occur when a device has been restarted,  
25 inactive, or has not been unlocked for a certain period of time. For example, Apple  
26 devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed  
27 since the device was last unlocked or (2) when the device has not been unlocked using a  
28 fingerprint for 4 hours and the passcode or password has not been entered in the last 156

1 hours. Biometric features from other brands carry similar restrictions. Thus, in the event  
2 law enforcement personnel encounter a locked device equipped with biometric features,  
3 the opportunity to unlock the device through a biometric feature may exist for only a  
4 short time.

5 58. Due to the foregoing, if law enforcement personnel encounter a device that  
6 is subject to search and seizure pursuant to this warrant and may be unlocked using one  
7 of the aforementioned biometric features, the warrant I am applying for would permit law  
8 enforcement personnel to (1) press or swipe the fingers (including thumbs) of  
9 C.S. CRAWFORD, who is found at the subject premises and reasonably believed by law  
10 enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold  
11 the device in front of his face and activate the facial recognition feature, for the purpose  
12 of attempting to unlock the device in order to search its contents as authorized by this  
13 warrant. In depressing a person's thumb or finger onto a device and in holding a device in  
14 front of a person's face, law enforcement may not use excessive force, as defined in  
15 *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more  
16 than objectively reasonable force in light of the facts and circumstances confronting  
17 them.

#### 18 SEARCH TECHNIQUES

19 59. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal  
20 Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,  
21 or otherwise copying digital devices or other electronic storage media that reasonably  
22 appear capable of containing some or all of the data or items that fall within the scope of  
23 Attachment B to this Affidavit, and will specifically authorize a later review of the media  
24 or information consistent with the warrant.

25 60. Because **TR1** may be a residence shared by C.S. CRAWFORD with other  
26 people, it is possible that **TR1** will contain digital devices or other electronic storage  
27 media that are predominantly used, and perhaps owned, by persons who are not suspected  
28 of a crime. If agents conducting the search nonetheless determine that it is possible that

the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

61. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

**A. Processing the Search Sites and Securing the Data**

62. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

63. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit.<sup>3</sup>

---

<sup>3</sup> The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

1           64. A forensic image may be created of either a physical drive or a logical  
2 drive. A physical drive is the actual physical hard drive that may be found in a typical  
3 computer. When law enforcement creates a forensic image of a physical drive, the image  
4 will contain every bit and byte on the physical drive. A logical drive, also known as a  
5 partition, is a dedicated area on a physical drive that may have a drive letter assigned (for  
6 example the c: and d: drives on a computer that actually contains only one physical hard  
7 drive). Therefore, creating an image of a logical drive does not include every bit and byte  
8 on the physical drive. Law enforcement will only create an image of physical or logical  
9 drives physically present on or within the subject device. Creating an image of the  
10 devices located at the search locations will not result in access to any data physically  
11 located elsewhere. However, digital devices or other electronic storage media at the  
12 search locations that have previously connected to devices at other locations may contain  
13 data from those other locations.

14           65. If based on their training and experience, and the resources available to  
15 them at the search site, the search team determines it is not practical to make an on-site  
16 image within a reasonable amount of time and without jeopardizing the ability to  
17 accurately preserve the data, then the digital devices or other electronic storage media  
18 will be seized and transported to an appropriate law enforcement laboratory to be  
19 forensically imaged and reviewed.

20 **A. Searching the Forensic Images**

21           66. Searching the forensic images for the items described in Attachment B may  
22 require a range of data analysis techniques. In some cases, it is possible for agents and  
23 analysts to conduct carefully targeted searches that can locate evidence without requiring  
24 a time-consuming manual search through unrelated materials that may be commingled  
25 with criminal evidence. In other cases, however, such techniques may not yield the  
26 evidence described in the warrant, and law enforcement may need to conduct more  
27  
28

1 extensive searches to locate evidence that falls within the scope of the warrant. The  
2 search techniques that will be used will be only those methodologies, techniques and  
3 protocols as may reasonably be expected to find, identify, segregate and/or duplicate the  
4 items authorized to be seized pursuant to Attachment B to this affidavit. Those  
5 techniques, however, may necessarily expose many or all parts of a hard drive to human  
6 inspection in order to determine whether it contains evidence described by the warrant.

7 **PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION**

8 67. As described above, I have obtained information regarding the Target  
9 Offenses through search warrants I obtained for information in the possession of the  
10 following providers of electronic communications services: Google LLC, Meta  
11 Platforms, Inc. (parent company of Facebook and Instagram), Amazon.com, and MG  
12 Freesites, Ltd. (parent company of Pornhub.com). Law enforcement review of the  
13 information received pursuant to these search warrants is still underway, though in some  
14 cases I have been able to corroborate some of the information I gathered from witnesses  
15 through the information received in response to the search warrants from the electronic  
16 communications services providers. The information I seek in the present search warrant  
17 would serve additional purposes, including: to link C.S. CRAWFORD to the evidence of  
18 cyberstalking and harassing communications and to the sources of those communications;  
19 to search for likely additional communications and evidence of cyberstalking not  
20 included in the information provided by the providers, and to obtain additional evidence  
21 of C.S. CRAWFORD's knowledge, intent, motive, identity, opportunity, and plan in  
22 committing the Target Offenses.

23 **REQUEST FOR SEALING**

24 68. It is respectfully requested that this Court issue an order sealing, until  
25 further order of the Court, all papers submitted in support of this application, including  
26 the application and search warrant. I believe that sealing this document is necessary  
27 because the items and information to be seized are relevant to the investigation into the  
28 criminal activity of C.S. CRAWFORD which will still be ongoing. Based upon my



1 training and experience, I have learned that, online criminals actively search for criminal  
2 affidavits and search warrants via the Internet and disseminate them to other online  
3 criminals as they deem appropriate, i.e., post them publicly online through various  
4 forums. Premature disclosure of the contents of this affidavit and related documents may  
5 have a significant and negative impact on the continuing investigation and may severely  
6 jeopardize its effectiveness.

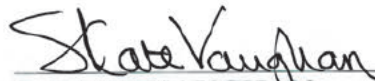
7 **CONCLUSION**

8 69. Based on the information set forth herein, I submit that this affidavit  
9 supports probable cause for a warrant to search **TR1** as described in Attachment A-1, the  
10 vehicle described in Attachment A-2, and the person of C.S. CRAWFORD described in  
11 Attachment A-3, for evidence and instrumentalities, as described in Attachment B, of the  
12 crimes of cyberstalking, in violation of 18 U.S.C. § 2261A(2)(B), and repeated harassing  
13 interstate communications, in violation of 47 U.S.C. § 223(a)(1)(E).

14  
15  
16 

17 EDDY D CROCHETIERE, Affiant  
18 Special Agent  
19 Naval Criminal Investigative Service

20 The above-named agent provided a sworn statement attesting to the truth of the  
21 contents of the foregoing affidavit by telephone on the 27th day of May 2022.

22  
23  
24 

25 S. KATE VAUGHAN  
26 United States Magistrate Judge  
27  
28

**ATTACHMENT A-1****Description of Property to Be Searched**

The property to be searched is a residence located at **8620 8th Avenue West, Apartment C, Everett, Washington 98204** (“the Target Residence 1” or “TR1”). TR1 is the apartment designated as Apartment C within a light blue/gray-colored two-story four-unit apartment building with two garage doors facing the street on the west side of 8th Avenue West in Everett (pictured below, left). The entrance to Apartment C is accessed by stairs to a door on the north side of the building (pictured below, right), and has a “C” on the door.



**ATTACHMENT A-2**

**Description of Vehicle to Be Searched**

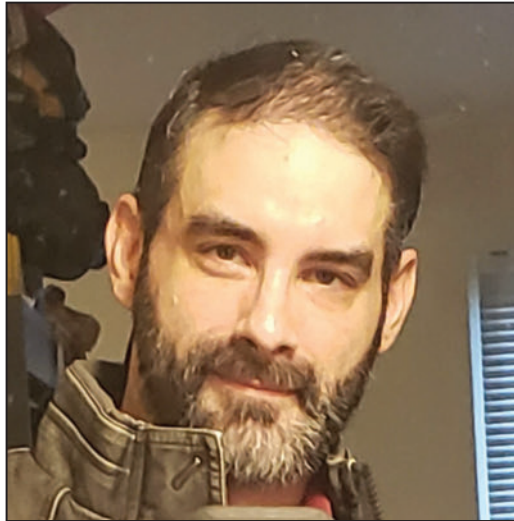
The vehicle to be searched is a silver Ford Ecosport with Washington state license plate number BPT0800 (pictured below), provided the vehicle is situated within the Western District of Washington.



**ATTACHMENT A-3**

**Description of Person to Be Searched**

The person to be searched is the person of Christopher Scott CRAWFORD, date of birth [REDACTED], 1980, provided he is situated within the Western District of Washington. C.S. CRAWFORD is a white male approximately 6 feet 2 inches tall, weighing approximately 160 pounds. A photograph of the person to be searched is below.





**ATTACHMENT B****Items to be Seized**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of cyberstalking, in violation of 18 U.S.C. § 2261A(2)(B), and repeated harassing interstate communications, in violation of 47 U.S.C. § 223(a)(1)(E) (the Target Offenses):

1. All records relating to the Target Offenses, those violations involving Christopher Scott CRAWFORD and occurring from April 1, 2019, to the present, including:

a. All records of electronic or telephonic communications, whether in written or audio form, including the substance of such communications, relating to the Target Offenses listed above;

b. Any written or electronically stored communications to or from the following individuals described in the application for this search warrant: K.C., D.A., M.N., J.M., or any family member or associate of K.C.;

c. Any communications to any email address affiliated with the United States Navy;

d. Records of internet searches related to the individuals in para. 1.b., above, including records contained in caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;

e. Images of K.C. or any of the individuals in para.1.b., above;

f. Any records of the sending or receiving of images of K.C. through

1 any messaging means or application, and any communications related to the possession,  
2 receipt, or transfer of images of K.C.;

3 g. Records related to the access of pornhub.com website, any account  
4 related to that website, and/or the transfer of files to that website;

5 h. Any records related to the use of the following email accounts:

6 i. crawford132@gmail.com;

7 ii. rickjohnston1888@gmail.com;

8 iii. endless sadness15@gmail.com;

9 i. Any records related to the use of the following Facebook accounts:

10 iv. Display name "Rick Johnston," account identifier  
11 100074078874761;

12 v. Display name "Scott Crawford," account identifier  
13 100002445195272;

14 vi. Display name "Christopher Crawford," account identifier  
15 100054164457078;

16 i. Any records related to the use of the following Instagram accounts:

17 vii. Display name "cscottcrawford," account identifier  
18 27235979350;

19 viii. Display name "'im\_not\_broken\_just\_very\_sad,'" account  
20 identifier 27605029014;

21 j. Any records or court documents related to the issuance or service of  
22 any restraining order, protective order, or no-contact order restraining the activities of  
23 Christopher Scott CRAWFORD;



2. Digital devices<sup>1</sup> or other electronic storage media<sup>2</sup> and/or their components, which include:

a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or

---

<sup>1</sup> “Digital device” includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants (“PDAs”), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

<sup>2</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1 data; and

2 g. Any passwords, password files, test keys, encryption codes or other  
3 information necessary to access the computer equipment, storage devices or data.

4 3. Any digital devices or other electronic storage media that were or may have  
5 been used as a means to commit the Target Offenses described on the warrant.

6 4. For any digital device or other electronic storage media upon which  
7 electronically stored information that is called for by this warrant may be contained, or  
8 that may contain things otherwise called for by this warrant:

9 a. evidence of who used, owned, or controlled the digital device or  
10 other electronic storage media at the time the things described in this warrant were  
11 created, edited, or deleted, such as logs, registry entries, configuration files, saved  
12 usernames and passwords, documents, browsing history, user profiles, email, email  
13 contacts, "chat," instant messaging logs, photographs, and correspondence;

14 b. evidence of software that would allow others to control the digital  
15 device or other electronic storage media, such as viruses, Trojan horses, and other forms  
16 of malicious software, as well as evidence of the presence or absence of security software  
17 designed to detect malicious software;

18 c. evidence of the lack of such malicious software;

19 d. evidence of the attachment to the digital device of other storage  
20 devices or similar containers for electronic evidence;

21 e. evidence of counter-forensic programs (and associated data) that are  
22 designed to eliminate data from the digital device or other electronic storage media;

23 f. evidence of the times the digital device or other electronic storage  
24 media was used;

25 g. passwords, encryption keys, and other access devices that may be  
26 necessary to access the digital device or other electronic storage media;

27 h. documentation and manuals that may be necessary to access the  
28 digital device or other electronic storage media or to conduct a forensic examination of

1 the digital device or other electronic storage media;

2 i. contextual information necessary to understand the evidence  
3 described in this attachment.

4 5. Records and things evidencing the use of an Internet Protocol address  
5 2601:601:a300:4ab0:cd57:98ec:2a4a:6899 to access the internet including:

6 a. routers, modems, and network equipment used to connect computers  
7 to the internet;

8 b. records of internet protocol addresses used;

9 c. records of internet activity, including firewall logs, caches, browser  
10 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user  
11 entered into any internet search engine, and records of user-typed web addresses.

12  
13 In depressing a person's thumb or finger onto a device and in holding a device in  
14 front of a person's face, law enforcement may not use excessive force, as defined in  
15 *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more  
16 than objectively reasonable force in light of the facts and circumstances confronting  
17 them.

18  
19 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE  
20 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS  
21 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO  
22 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC  
23 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL  
24 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE  
25 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR  
26 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED  
27 CRIMES  
28